

Application Serial No. 09/773,535

Attorney Docket No. 52493.000152

The Listing of Claims:

1. (Currently amended) A method for transmitting data comprising:

placing a file in a destination based transmit folder;

retrieving a the file from a the destination based transmit folder;

encrypting the file with an a particular encryption process associated with the destination based transmit folder including determining the particular encryption process by which the file is to be encrypted, the determining being based on what destination based transmit folder the file was retrieved from in such manner that the destination based transmit folder dictates the particular encryption process; and

transmitting the file to an outgoing folder for transmission to a destination, which is associated with the destination based transmit folder; and

wherein the particular encryption process converts the file from one data set to an encrypted data set, access to the file being precluded while the file is encrypted.

2. (Original) The method of claim 1 further comprising retrieving the encryption process associated with the destination based transmit folder from an encryption database.
3. (Original) The method of claim 1 further comprising verifying that the file has been encrypted.
4. (Original) The method of claim 3 wherein verifying that the file has been encrypted comprises transferring the file to a temporary folder and checking if all files in the temporary folder have been encrypted.
5. (Original) The method of claim 3 further comprising moving the file to an error directory if the file fails the verification process.

Application Serial No. 09/773,535

Attorney Docket No. 52493.000152

6. (Original) The method of claim 3 further comprising recording information about the file in an error log if the file fails the verification process.
7. (Original) The method of claim 6 further comprising transmitting a destination based portion of the error log to the destination.
8. (Original) The method of claim 3 wherein transmitting the file to the outgoing folder comprises transmitting the verified file to the outgoing folder.
9. (Original) The method of claim 3 further comprising transmitting notification of verification failure of the file to the destination if the file fails verification.
10. (Original) The method of claim 1 further comprising transmitting notification of encryption failure of the file to the destination if the file fails encryption.
11. The method of claim 1 further comprising moving the file to an error directory if the file fails the encryption process.
12. (Original) The method of claim 1 further comprising recording information about the file in an error log if the file fails the encryption process.
13. (Original) The method of claim 1 further comprising:
 - retrieving the file from the outgoing box;
 - transmitting the file to the destination; and
 - verifying receipt of the file at the destination.
14. (Original) The method of claim 1 further comprising receiving the file in the destination based transmit folder wherein a user selects a file destination and places the file in the destination based transmit folder corresponding to the file destination.

Application Serial No. 09/773,535

Attorney Docket No. 52493.000152

15. (Original) The method of claim 1 wherein retrieving the file from the destination based transmit folder comprises automatically checking the destination based transmit folder for new files after a predetermined time interval and retrieving new files found in the destination based transmit folder.
16. (Original) The method of claim 1 further comprising transmitting the encrypted file.
17. (Original) The method of claim 1 further comprising transmitting the encrypted file over an insecure channel.
18. (Original) The method of claim 1 wherein the encryption process comprises a public key for encoding the file.
19. (Original) The method of claim 1 further comprising generating a file notifying a recipient at the destination that the file is being transmitted.
20. (Original) The method of claim 1 further comprising performing a scan for encryption key software to find the encryption process.
21. (Previously presented) The method of claim 1 further comprising transmitting a list of files from the destination based transmit folder to the outgoing folder to reconcile files being transferred from the destination based transmit folder to the outgoing folder.
22. (Original) The method of claim 1 further comprising compressing the data.
23. (Currently amended) A system for transmitting data comprising:
- means for storing a file in a destination based transmit folder;
- means for retrieving a file from a destination based transmit folder;
- means for encrypting the file with a particular encryption process associated with the destination based transmit folder, the encrypting including determining the particular encryption process by which the file is to be encrypted, the determining being based on what destination

Application Serial No. 09/773,535

Attorney Docket No. 52493.000152

based transmit folder the file was retrieved from in such manner that the destination based transmit folder dictates the particular encryption process; and

means for transmitting the file to an outgoing folder for transmission to the destination, which is associated with the destination based transmit folder; and

wherein the particular encryption process converts the file from one data set to an encrypted data set, access to the file being precluded while the file is encrypted.

24. (Original) The system of claim 23 further comprising means for retrieving the encryption process associated with the destination based transmit folder from an encryption database.

25. (Previously presented) The system of claim 23 further comprising means for verifying that the file has been encrypted.

26. (Previously presented) The system of claim 23 further comprising:

means for retrieving the file from the outgoing folder;

means for transmitting the file to the destination; and

means for verifying receipt of the file at the destination.

27. (Currently amended) A method for receiving data comprising:

placing a file in a destination based received folder

retrieving ~~a~~ the file from ~~a~~ the destination based received folder;

decrypting the file with a particular decryption process associated with the destination based received folder, including determining the particular decryption process by which the file is to be decrypted, the determining being based on what destination based received folder the file

Application Serial No. 09/773,535

Attorney Docket No. 52493.000152

was retrieved from in such manner that the destination based received folder dictates the particular decryption process; and

transmitting the file to an outgoing folder for access at a destination, which is associated with the destination based received folder; and

wherein the particular decryption process converts the file from an encrypted data set to a decrypted data set, access to the file being precluded while the file is encrypted.

28. (Original) The method of claim 27 further comprising retrieving the decryption process associated with the destination based received folder from a decryption database.

29. (Original) The method of claim 27 further comprising verifying that the file has been decrypted.

30. (Original) The method of claim 29 wherein verifying that the file has been decrypted comprises transferring the file to a temporary folder and checking if all files in the temporary folder have been decrypted.

31. (Original) The method of claim 29 further comprising moving the file to an error directory if the file fails the verification process.

32. (Original) The method of claim 29 further comprising recording information about the file in an error log if the file fails the verification process.

33. (Original) The method of claim 32 further comprising transmitting a destination based portion of the error log to the destination.

34. (Original) The method of claim 29 wherein transmitting the file to the outgoing folder comprises transmitting the verified file to the outgoing folder.

35. (Original) The method of claim 29 further comprising transmitting notification of decryption failure of the file to the destination if the file fails verification.

Application Serial No. 09/773,535

Attorney Docket No. 52493.000152

36. (Original) The method of claim 27 further comprising transmitting notification of decryption failure of the file to the destination if the file fails decryption.
37. (Original) The method of claim 27 further comprising moving the file to an error directory if the file fails the decryption process.
38. (Original) The method of claim 27 further comprising recording information about the file in an error log if the file fails the decryption process.
39. (Original) The method of claim 27 wherein retrieving the file from the destination based received folder comprises automatically checking the destination based received folder for new files after a predetermined time interval and retrieving new files found in the destination based received folder.
40. (Original) The method of claim 27 further comprising receiving the file in a file received inbox and placing the file in the destination based received folder.
41. (Original) The method of claim 40 wherein receiving the file comprises receiving the file over an insecure channel.
42. (Original) The method of claim 41 wherein placing the file in the appropriate destination based received folder comprises determining the destination of the file.
43. (Original) The method of claim 27 wherein the decryption process comprises a private key for decoding the file.
44. (Original) The method of claim 27 further comprising performing a scan for decryption key software to find the decryption process.
45. (Previously presented) The method of claim 27 further comprising transmitting a list of files from the destination based received folder to the outgoing folder to reconcile files being transferred from the destination based received folder to the outgoing folder.

Application Serial No. 09/773,535

Attorney Docket No. 52493.000152

46. (Original) The method of claim 27 further comprising decompressing the data.

47. (Currently amended) A system for receiving data comprising:

means for storing a file in a destination based received folder;

means for retrieving ~~a~~the file from ~~a~~the destination based received folder;

means for decrypting the file with a decryption process associated with the destination based received folder, the decrypting including determining the particular decryption process by which the file is to be decrypted, the determining being based on what destination based received folder the file was retrieved from in such manner that the destination based received folder dictates the particular decryption process; and

means for transmitting the file to an outgoing folder for access at a destination, which is associated with the destination based received folder; and

wherein the particular decryption process converts the file from an encrypted data set to a decrypted data set access to the file being precluded while the file is encrypted.

48. (Original) The system of claim 47 further comprising means for retrieving the decryption process associated with the destination based received folder from an encryption database.

49. (Previously presented) The system of claim 47 further comprising means for verifying that the file has been decrypted.

50. (Previously presented) The system of claim 47 further comprising means for receiving the file in a file received inbox and placing the file in the destination based received folder.

51. (Currently amended) A method for transmitting data comprising:

placing data in a destination based transmit folder;

automatically retrieving the data from ~~a~~the destination based transmit folder;

Application Serial No. 09/773,535

Attorney Docket No. 52493.000152

automatically retrieving ~~an a particular~~ encryption process associated with the destination based transmit folder, the retrieving including determining the particular encryption process by which the data is to be encrypted, the determining being based on what destination based transmit folder the data was retrieved from in such manner that the destination based transmit folder dictates the particular encryption process;

encrypting the data with the particular encryption process; and

transmitting the data to an outgoing folder for transmission to a destination, which is associated with the destination based transmit folder; and

wherein the particular encryption process converts the data from one data set to an encrypted data set, access to the data being precluded while the data is encrypted.

52. (Original) The method of claim 51 wherein the encryption process comprises an encryption key.

53. (Original) The method of claim 51 further comprising transferring the data to a temporary folder to verify that the data has been encrypted.

54. (Original) The method of claim 51 further comprising performing error processing on the data if the data fails verification.

55. (Original) The method of claim 51 further comprising performing error processing on the data if the data fails encryption.

56. (Currently amended) A system for transmitting data comprising:

means for storing data in a destination based transmit folder;

means for automatically retrieving the data from ~~a the~~ destination based transmit folder;

means for automatically retrieving ~~an a particular~~ encryption process associated with the destination based transmit folder, the retrieving including determining the particular encryption

Application Serial No. 09/773,535

Attorney Docket No. 52493.000152

process by which the data is to be encrypted, the determining being based on what destination based transmit folder the data was retrieved from in such manner that the destination based transmit folder dictates the particular encryption process;

means for encrypting the data with the encryption process; and

means for transmitting the data to an outgoing folder for transmission to a destination, which is associated with the destination based transmit folder; and

wherein the particular encryption process converts the data from one data set to an encrypted data set, access to the data being precluded while the data is encrypted.

57. (Original) The system of claim 56 wherein the encryption process comprises an encryption key.

58. (Original) The system of claim 56 further means for comprising transferring the data to a temporary folder to verify that the data has been encrypted.

59. (Original) The system of claim 58 further comprising means for performing error processing on the data if the data fails verification.

60. (Previously presented) The system of claim 58 further comprising means for performing error processing on the data if the data fails encryption.

61. (Currently amended) A method for receiving data comprising:

automatically placing received data in a destination based received folder;

automatically retrieving data from the destination based received folder;

automatically retrieving a particular decryption process associated with the destination based received folder, the retrieving including determining the particular decryption process by which the data is to be decrypted, the determining being based on what destination based

Application Serial No. 09/773,535

Attorney Docket No. 52493.000152

received folder the data was retrieved from in such manner that the destination based received folder dictates the particular decryption process;

decrypting the data with the particular decryption process; and

transmitting the data to an outgoing folder for access at a destination, which is associated with the destination based received folder; and

wherein the particular decryption process converts the data from an encrypted data set to a decrypted data set, access to the data being precluded while the data is encrypted.

62. (Previously presented) The method of claim 61 wherein the decryption process comprises an decryption key.

63. (Original) The method of claim 61 further comprising transferring the data to a temporary folder to verify that the data has been decrypted.

64. (Canceled)

65. (Canceled)

66. (Currently amended) A system for receiving data comprising:

means for automatically placing received data in a destination based received folder;

means for automatically retrieving data from the destination based received folder;

means for automatically retrieving a particular decryption process associated with the destination based received folder, the retrieving including determining the particular decryption process by which the data is to be decrypted, the determining being based on what destination based received folder the data was retrieved from in such manner that the destination based received folder dictates the particular decryption process;

means for decrypting the data with the particular decryption process; and

Application Serial No. 09/773,535

Attorney Docket No. 52493.000152

means for transmitting the data to an outgoing folder for access at a destination, which is associated with the destination based received folder; and

wherein the particular decryption process converts the data from an encrypted data set to a decrypted data set, access to the data being precluded while the data is encrypted.

67. (Previously presented) The system of claim 66 wherein the decryption process comprises an decryption key.

68. (Original) The system of claim 66 further comprising means for transferring the data to a temporary folder to verify that the data has been decrypted.

69. (Original) The system of claim 68 further comprising means for performing error processing on the data if the data fails verification.

70. (Original) The system of claim 66 further comprising means for performing error processing on the data if the data fails decryption.

71. (Currently amended) An automatic encryption system for data to be transmitted comprising:

an encryption module receiving data in a destination based transmit folder and automatically encrypting the data with ~~an a particular~~ encryption method associated with the destination based transmit folder, the automatically encrypting including determining the particular encryption process by which the data is to be encrypted, the determining being based on what destination based transmit folder the data was retrieved from in such manner that the destination based transmit folder dictates the particular encryption process;

an encryption database storing encryption methods, including the particular encryption method, each encryption method associated with at least one destination based transmit folder;

an error module performing error processing on data failing encryption; and

Application Serial No. 09/773,535

Attorney Docket No. 52493.000152

wherein the particular encryption process converts the data from one data set to an encrypted data set, access to the data being precluded while the data is encrypted.

72. (Original) The system of claim 71 further comprising a file compression module compressing the data to be transmitted.

73. (Original) The system of claim 71 wherein the encryption module comprises a verification module verifying encryption of the data.

74. **(Currently amended)** An automatic decryption system for received data comprising:

a decryption module receiving data in a destination based received folder and automatically decrypting the data with a particular decryption method associated with the destination based received folder, the automatically decrypting including determining the particular decryption method by which the data is to be decrypted, the determining being based on what destination based transmit folder the file was retrieved from in such manner that the destination based received folder dictates the particular encryption method;

a decryption database storing decryption methods, including the particular decryption process, each decryption method associated with at least one destination based received folder;

an error module performing error processing on data failing decryption; and

wherein the particular decryption process converts the data from an encrypted data set to a decrypted data set, access to the data being precluded while the file is encrypted.

75. (Original) The system of claim 74 further comprising a file decompression module decompressing the received data.

76. (Original) The system of claim 74 wherein the decryption module comprises a verification module verifying decryption of the data.

77. **(Canceled)**

Application Serial No. 09/773,535

Attorney Docket No. 52493.000152

78. **(Previously presented)** The method of claim 1, wherein the determining is performed after the file is retrieved from the destination based transmit folder.